REMARKS

Claims 1-3, 5-11, 14-16, and 18-28 are currently pending in the subject application and are presently under consideration. Claims 1, 14, 18, 22, 26 and 27 have been amended as shown on pages 2-6 of the Reply. Applicants' representative thanks the Examiner for the teleconference of October 8, 2008 wherein merits of the claims vis-à-vis the cited art were discussed. The Examiner indicated that the claim amendments seemed to overcome existing rejections and necessitate further search.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 22-25 Under 35 U.S.C §112

Claims 22-25 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 22 has been amended herein. In view of the amendments, this rejection is now moot and should be withdrawn.

II. Rejection of Claims 1-5, 9, 10, 12-21, 26, and 27 Under 35 U.S.C. §102(b)

Claims 1-5, 9, 10, 12-21, 26, and 27 stand rejected under 35 U.S.C. §102(b) as being anticipated by Stallings (*Cryptography and Network Security; Third Edition.* Chapter 9 / Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems). Withdrawal of this rejection is requested for the following reasons. The cited reference fails to disclose or suggest all aspects set forth in the subject claims.

> A single prior art reference anticipates a patent claim only if it ***expressly or inherently describes each and every limitation set forth in the patent claim***. *Trintec Industries, Inc. v. Top-U.S.A. Corp.*, 295 F.3d 1292, 63 USPQ2d 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California,* 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The ***identical invention must be shown in as complete detail as is contained in the … claim***. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (emphasis added).

Applicants' claimed subject matter provides methods and systems facilitating the exchange and use of a session key to facilitate secure communication. The session key along with asymmetric encryption is utilized to send an encrypted message comprising a digital certificate, the certificate is utilized to create a remote service binding of the initiator of the message in the system of the target of the message. To this end amended independent claim 1 recites *a message encryption system comprising: a session key employed to securely exchange a message associated with a dialog; and, an encryption component that employs asymmetric encryption to first securely transmit the session key, the session key thereafter being employed to encrypt the message and securely exchange the message, wherein the session key encrypted message is further encrypted using a private key securely associated with an initiator of the message,* ***the message comprises a digital certificate that is employed as part of a service broker security system that facilitates location transparency of services by creating a remote service binding which addresses a service by a logical name such that an application can utilize the service independent of the physical location of the service.*** Independent claims 14, 18 and 26 recite similar features. Independent claim 27 recites ***means for employing a digital certificate included in the message to create a remote service binding such that an application can utilize the service independent of the physical location of the service.*** Stallings is silent regarding such claimed features.

Stallings relates to principles of public-key cryptosystems and secret key distribution with confidentiality and authentication. At the cited portions, Stallings discloses a secret key distribution that provides protection against both active and passive attacks. A secret key is encrypted using the private key-public key pair and passed from an initiator to a recipient. The encrypted message containing the secret key is decrypts the message to recover the secret key. Further, Stallings discloses that each session key is associated with a single message and is used for encrypting and decrypting the message. Nowhere does Stallings disclose regarding ***the message comprises a digital certificate that is employed as part of a service broker security system that facilitates location transparency of services by creating a remote service binding which addresses a service by a logical name such that an application can utilize the service independent of the physical location of the service.*** In contrast, the claimed invention allows for encrypting messages sent from the initiator, first with the session key then encrypted message again encrypted with the private key of the initiator. This message comprises a digital certificate

that is employed by a service broker security system that facilitates location transparency of services. The initiator and recipient of the message have a copy of each other's digital certificate comprising the public key and with appropriate permissions to send to services, they will be able to access the service regardless of where the service is actually located. However, Stallings is silent regarding the aforementioned features recited by the subject claims. Claim 10 recites ***the digital certificate being associated with a user via a login protocol.*** At the cited portions, Stallings discloses a digital certificate received from the certificate authority, the certificate is sent from an initiator to a recipient. The recipient uses the authority public key to read the message and verify it. However, Stallings is silent regarding ***the digital certificate being associated with a user via a login protocol*** as recited by claim 10. The claimed invention allows for the initiator of the message comprising the certificate, to access the service provided by the recipient regardless of where the service is actually located. Stallings does not disclose such novel features.

Additionally, Stallings fails to teach or suggest ***creating a remote service binding which addresses a service by a logical name such that an application can utilize the service independent of the physical location of the service***. By allowing services to be addressed logically by name, the system and method of the present invention allow applications to be built independent of where the service is located physically. At deployment time, the services can be moved to different physical locations without affecting the application.

Accordingly, it is requested that this rejection with respect to independent claims 1, 14, 18, 26 and 27 should be withdrawn.

III. Rejection of Claim 11 Under 35 U.S.C. §103(a)

Claim 11 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings (*Cryptography and Network Security; Third Edition.* Chapter 9 / Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems). It is respectfully requested that this rejection be withdrawn for at least the following reasons. Claim 11 depends from independent claim 1. As discussed supra, Stallings does not teach or suggest all aspects of amended independent claim 1. Accordingly, it is requested that this rejection be withdrawn.

IV. Rejection of Claims 6-8 and 22-25 Under 35 U.S.C. §103(a)

Claims 6-8 and 22-25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings in view of VanHeyningen *et al.* (US 2002/0112152). It is respectfully requested that this rejection be withdrawn for at least the following reasons. Stallings and VanHeyningen *et al.* do not teach or suggest all aspects set forth in the subject claims. Claims 6-8 depend from independent claim 1, and as discussed supra, Stallings does not teach or suggest all aspects recited by amended independent claim 1. VanHeyningen *et al.* discloses methods and apparatus for providing secure streaming data transmission facilities using unreliable protocols and does not compensate for the aforementioned deficiencies of Stallings. Independent claim 22 recites similar features as independent claim 1, namely ***facilitating location transparency of services within a service broker security system employing a digital certificate included in the subsequent message by creating a remote service binding which addresses a service by a logical name such that an application can utilize the service independent of the physical location of the service.*** VanHeyningen *et al.* does not disclose such features recited by independent claim 22.

Further, it is erroneously contended on page 10 of the subject Office Action, that VanHeyningen *et al.* discloses a system wherein multiple instances of the same service negotiate different session keys with different subscribers. At the cited portion, VanHeyningen *et al.* teaches a number of proxy servers being used by different client servers rather than multiple instances of a single service broker. Accordingly, it is respectfully submitted that this rejection should be withdrawn.

V. Rejection of Claim 28 Under 35 U.S.C. §103(a)

Claim 28 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings in view of Wasilewski *et al.* (US 5,870,474). It is respectfully requested that this rejection be withdrawn for at least the following reasons. Claim 28 depends from independent claim 1, and as discussed *supra*, Stallings does not teach or suggest all aspects recited by amended independent claim 1. Wasilewski *et al.* relates to a control system for providing secure transmission of information services such as video, audio, interactive games etc. between a service provider and a customer's set top unit over a digital network, and does not compensate for the aforementioned deficiencies of Stallings.

Additionally, it is erroneously contended on page 9 of the subject Office Action that Wasilewski *et al.* teaches multiple instances of a service broker sharing the same private key. At the cited portions, Wasilewski *et al.* teaches a single CAM (conditional access manager – which is the master of a conditional access system) and SABER (Service Access Broadband Encrypter and Remapper) being shared by different service providers. Hence, contrary to the claimed aspect wherein multiple instances of a service broker are utilized by different clients by sharing a private key associated with the service, Wasilewski *et al.* teaches a single CAM and/or SABER being shared by different service providers by sharing the same private key. These instances that share the same private key as the service are no different from the actual service hence no changes need to be made at the subscriber side when dealing with different instances. This facilitatates load balancing as the number of subscriber increases, additional instances can be deployed to share the load (*See* Fig. 8 and related text in section labeled 'Delegated handshake' of applicants' specification). Such load balancing would not be possible for the system disclosed by Wasilewski *et al.* wherein a single CAM and/or SABER is being shared by different service providers. Accordingly, it is respectfully submitted that this rejection should be withdrawn.

VI. Rejection of Claims 22-25 Under 35 U.S.C. §103(a)

Claims 22-25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings and VanHeyningen *et al.* (US 2002/0112152) in view of Wasilewski *et al.* (US 5,870,474). It is respectfully requested that this rejection be withdrawn for at least the following reasons. Claim 22 recites ***deploying multiple instances of the service broker;sharing the private key within the multiple instances of the service broker***. As discussed *supra*, Stallings and VanHeyningen and Wasilewski *et al.* do not teach or suggest such claim features. Accordingly, it is respectfully submitted that this rejection should be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP566US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731